



Gemeente Rotterdam

Servicedienst

Acceptatiecriteria

SSC ICT diensten

Auteur

SSC ICT diensten

Datum

17 maart 2010

Versie

1.4

Status



Documentbeheer

Historie van het document

Datum	Versie	Status	Change
18 maart 2010	0.1	Concept	Eerste samenvoeging acceptatiecriteria KCR en ICT services
30 maart 2010	1.0	Final	Eerste versie acceptatiecriteria SSC ICT diensten
28 juni 2010	1.1	Final	Actualisering
10 augustus 2010	1.2	Final	Aanpassing tekst CiTi
4 oktober 2010	1.3	Final	Update tekst CiTi (MSSQL)
17 maart 2011	1.4	Final	Tekstuele correctie in paragraaf 2.2



Inhoudsopgave

1.	Inleiding	4
1.1	Algemeen	4
2.	De ICT infrastructuur	6
2.1	Beschrijving ICT infrastructuur	6
2.2	Database omgevingen	8
3.	Rotterdamse richtlijnen	11
3.1	Informatiebeveiliging	11
3.2	Opensource en open standaarden	13
3.3	Gegevensuitwisseling	14
3.4	Gewenste Autorisatiemodel	15
4.	Acceptatiecriteria	17
4.1	Acceptatiecriteria technische infrastructuur en Rotterdamse richtlijnen	17
5.	Overdrachtcriteria intern IdR	19
5.1	Overdracht van software naar TAB	19
Bijlagen 20		



1. Inleiding

1.1 Algemeen

Dit document beschrijft de acceptatiecriteria die SSC ICT diensten (Servicedienst - IdR) stelt aan in beheer te nemen systemen of delen van systemen.

1.1.1 Gebruik

Het document dient te worden gebruikt door de volgende (groepen van) personen:

Actor	Toelichting
Afnemers, Informatiemanagers, opdrachtgevers	De acceptatiecriteria worden gehanteerd tijdens de <i>pakketselectie</i> (van nieuwe software). Ook ten behoeve van het programma van eisen in Europese <i>aanbestedingstrajecten</i> .
Projectleiders / Projectmanagers	Projecten dienen conform de acceptatiecriteria producten te <i>implementeren en op te leveren</i> .
Opdrachtgevers	Dit document is een deel van de basis voor de opdrachtgever om <i>decharge</i> te kunnen verlenen aan zijn leveranciers.
Opdrachtnemers	Dit document is een deel van de basis voor de opdrachtnemers om aantoonbaar te kunnen maken dat hij <i>levert conform afspraak</i> .
Architecten	Geeft inzicht op globaal niveau in de opbouw van de technische architectuur; een verdere uitdieping kan worden gevonden in het Technisch Ontwerp van de ICT architectuur
Overdracht, in beheer name intern IdR	In dit document zijn een aantal criteria opgenomen welke intern IdR worden gebruikt om werkzaamheden tussen afdelingen onderling over te dragen

1.1.2 Acceptatiecriteria

Acceptatiecriteria hebben tot doel het kunnen vaststellen of een Informatie(deel)systeem is gerealiseerd conform vooraf vastgestelde eisen en wensen. Deze wensen en eisen dienen in een zo vroeg mogelijk stadium bij de realiserende partij bekend te zijn zodat deze kunnen worden meegenomen in de ontwerp-, realisatie of aanschaf van een Informatie(deel)systeem. Op die manier wordt al bij aanvang duidelijk waar de uiteindelijke oplevering aan dient te gaan voldoen.

1.1.3 Structuur en positie van dit document ten opzichte van andere documenten

De in dit document gestelde criteria kunnen verwijzen naar diverse beleidskaders en geldende werkafspraken ten aanzien van het beheren van informatiesystemen. Daarbij wordt in dit document regelmatig verwezen naar documenten met standaarden.

1.1.4 Afspraken en timing

De in dit document gestelde criteria zijn niet limitatief. Dit betekent dat per oplevering afgesproken moet worden welke set van criteria van toepassing zijn en dus onderdeel uitmaken van de oplevering. Tevens moet van deze criteria worden vastgesteld op welke termijn (of gekoppeld aan prestatie) de relevante documenten beschikbaar zijn.



1.1.5 Opbouw

In hoofdstuk 2 wordt een korte beschrijving op hoofdlijnen gegeven van de technische architectuur. Hierna volgt in hoofdstuk 3 een aantal gemeentelijke richtlijnen welke de selectie en implementatie en in beheer name van applicaties 'technisch' raakt en daarmee thuishoren in de acceptatiecriteria van SSC ICT diensten. In hoofdstuk 4 worden vervolgens de bijbehorende criteria geformuleerd. Tot slot is in hoofdstuk 5 een aantal criteria toegevoegd welke van toepassing zijn bij overdracht van werkzaamheden tussen afdelingen intern SSC ICT diensten.

In de bijlage is de door SSC ICT diensten gehanteerde beheermodel opgenomen, waarin 4 vormen worden onderscheiden en toegelicht: functioneel beheer, functioneel applicatie beheer, technisch applicatie beheer en technisch beheer.



2. De ICT infrastructuur

2.1 Beschrijving ICT infrastructuur

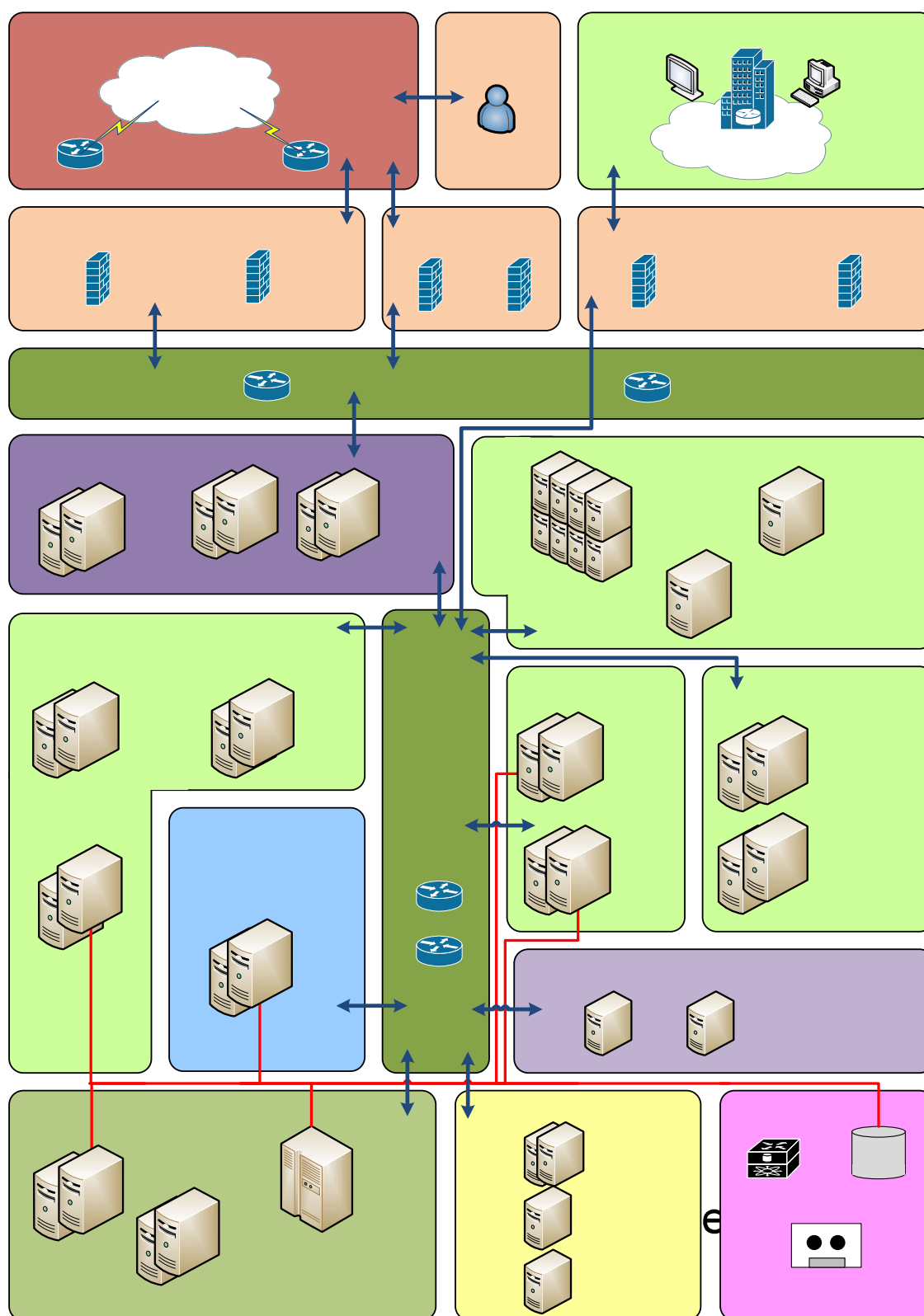
In Rotterdam is een technische ICT infrastructuur gerealiseerd die zich kenmerkt door een hoge betrouwbaarheid en schaalbaarheid. Deze infrastructuur wordt de 'CiTi' genoemd (spreek uit als city). CiTi staat voor Concern IT Infrastructuur en heeft als doel uiteindelijk de gehele gemeentelijke organisatie te voorzien van ICT middelen. In principe kan 7x24 uur gebruik worden gemaakt van de infrastructuur (serverzijde is altijd op, met uitzondering van een service window voor onderhoud, met wacht en waak dienst). De CiTi laat zich als volgt kenschetsen:

- er wordt gebruik gemaakt van 2 fysieke datacenters op geografische afstand in de stad (Galvanistraat en Hofdijk)
- de datacenters zijn onderling verbonden middels 6 glasvezelparen voor razendsnel datatransport
- alle data wordt gespiegeld tussen de 2 datacenters voor de basis en de plusdiensten
- toegang voor bedrijfskritische data met hoge beschikbaarheid wordt gerealiseerd op basis van Storage Area Network (SAN/NETAPP) systemen (in ieder datacenter is SAN/NETAPP apparatuur geplaatst)
- afhankelijk van de gewenste beschikbaarheid worden applicatie(servers) gespiegeld tussen de 2 datacenters
- er wordt gebruik gemaakt van bladeserver technologie
- er wordt gebruik gemaakt van virtualisatie op server, netwerk, applicatie en cliënt niveau
- de werkplekarchitectuur is gebaseerd op Server Based Computing (Citrix)
- de netwerk infrastructuur zal d.m.v. het toepassen van vlan's per taak/functie worden gescheiden
- voor het WAN wordt gebruik gemaakt van het Intranet * Rotterdam
- klantlocaties worden ontsloten via Intranet * Rotterdam. Daarbij varieert de beschikbare bandbreedte tussen de 2 Mbit en 1 Gbit en worden proxy en firewalls gebruikt
- "any time, any place" is de CiTi toegankelijk, vanuit de private cloud wordt op een veilige wijze een 'full desktop', Outlook web acces, Outlook mobile Acces aangeboden.
- Het ontwerp sluit aan bij de SOA architectuur van de Gemeente Rotterdam (OIM/DMC) en voldoet op hoofdlijnen aan de in NORA v2 gestelde richtlijnen voor infrastructuren binnen de overheid. Hierdoor is een toekomstvastheid van 4-7 jaar gegarandeerd.

De volgende softwareproducten zijn in de CiTi toegepast :

- Microsoft Windows Server als basis Operating System (standaard 64bit indien nodig 32 bit), hierop kan indien nodig worden afgeweken.
- Microsoft Exchange als mail oplossing
- Microsoft Forefront security for Exchange beveiligt en controleert de mail flow binnen het netwerk.
- Active Directory service voor autorisatie en authenticatie.
- Citrix access gateway appliances t.b.v. remote access.
- Het cisco 6500 platform t.b.v. routing en switching (virtual switch system)
- Microsoft ISA server om internet toegang te controleren en te reguleren.
- VMware ESX voor server virtualisatie beheerd vanuit Virtualcenter .
- Image distributie via Altiris, applicatiedistributie middels Citrix Presentation server, Softricity, Powerfuse.
- Backup HP Data Protector Software, HP Virtual Library Systeem VLS6653, ESL712e Ultrium Tape Library.

In onderstaande figuur is de CiTi weergegeven:





Gebruikte standaardset (core) kantoor automatisering applicaties in de CiTi (NB: in de oude IT omgevingen worden andere versies gebruikt):

Core Applicaties 21.100	
Windows XP SP3	
Calculator	
Kladblok	
Paint	
Windows verkenner	
MS Internet Explorer 7	
Microsoft Office Professional Editie 2003	
Word 2003	11.8169.8172 SP3
Excel 2003	11.8012.6360 SP1
Powerpoint 2003	11.8024.6360 SP1
Publisher 2003	11.6255.6360 SP1
Outlook 2003	11.8002.6360. SP1
InfoPath 2003	11.6357.6360. SP1
Adobe Reader 8.1.0	
CutePDF Writer 2.7	
Telefoongids (link voor KPN website)	
MS MediaPlayer 10	
Citrix ICA Client 10.200	
Oracle Client 10g Release 2 (10.2.0.1.0)	
Electronische Groene Boekje 3.0	
FlashPlayer 9.0.1	
McAfee 8.5.0 i	
Powerfuse Desktop Client 8.02	

2.2 Database omgevingen

Ten behoeve van databaseomgevingen is zowel voorzien in een algemene *Oracle* voorziening als een *MSSQL* voorziening. Bij voorkeur wordt gebruik gemaakt van het Oracle platform.

Oracle Platform

Gezien de hoeveelheid te ondersteunen databases is het Red Hat enterprise server (64bit) als basis Operating System (OS) toegepast. Alle database servers zijn voorzien van dezelfde versie van het OS tenzij er voor een specifieke Oracle RDBMS versie expliciet een OS versie noodzakelijk is. Er kunnen situaties voorkomen dat een pakketleverancier in de definitie van eisen expliciet om een OS vraagt. Voorbeeld hiervan kan bijvoorbeeld een Windows database server zijn. Deze passen in de voorgestelde architectuur, maar worden niet als standaard beschouwd.

Op dit moment is Oracle geïnstalleerd op zes nodes (servers). Hier kunnen 'hot pluggable' meer nodes aan worden toegevoegd. Per cluster is database functionaliteit geleverd in een Active/Active wijze door toepassing van RAC (Oracle Real Application Cluster). Het RAC Cluster draait op (l)unix 64bin nodes. Deze zullen vooraf geïnstalleerd worden met de door Oracle gevraagde kernel parameters, settings en user. Via de Oracle Clusterware software worden alle nodes waaruit het RAC-Cluster bestaat automatisch gezien.

Binnen de gemeente infrastructuur worden de laatste 2 major Oracle releases ondersteund. Dit zijn op dit moment Oracle10Gr2 en Oracle11G. Eerdere versies Oracle8i/9i kunnen ondersteund worden, maar vallen buiten deze scope.

Databases zijn onder te verdelen in Online Transaction Process en Datawarehousing databases. Dit



vereist specifieke configuratie van de omgeving. Er zijn aparte nodes voor OLTP en DWH databases. In geval van calamiteit kan hiervan afgeweken worden.

Ten behoeve van het Oracle RAC wordt shared storage gebruikt. Deze storage is via het SAN/NETAPP beschikbaar gesteld en vrijwel onbeperkt uitbreidbaar. Het SAN/NETAPP kan op meerdere manieren de storage aanbieden.

Indien client software niet 100% geschikt is voor een Active/Active connectie met load balancing ondersteunt Oracle RAC ook nog een expliciete toewijzing van een applicatie aan een node. Mocht er dan iets met een node gebeuren, kan via Transparent Application failover de connectie automatisch verlegd worden. Per applicatie zal uitgezocht moeten worden welke connectie mode gebruikt kan worden.

Afhankelijk van de benodigde database opties in een database, maakt Oracle users aan. Deze users zullen standaard in verband met security gelocked worden. De DBA-ers hebben een expliciet account voor de beheerswerkzaamheden met de benodigde rechten. De diverse applicaties worden binnen de applicatie schema's aangemaakt, welke niet gebruikt worden binnen de applicaties. Afhankelijk van het type applicatie zullen applicatie gebruikers aangemaakt worden en met de juiste set aan rechten. De applicatie schema's zullen gelocked worden om misbruik te voorkomen.

Om vanuit een client toegang te krijgen tot het RAC-Cluster dient de SQL-Net configuratie. Per dienst zal mogelijk een SQL-Net configuratie noodzakelijk zijn omdat niet iedere dienst bij iedere database kan/mag komen. SQL-Net ondersteunt ODBC, JDBC, LDAP names resolutie. LDAP naming resolutie heeft de voorkeur gezien het aantal diensten, redundantie en beheersgemak daar waar mogelijk.

MSSQL platform

Het SQL 2005 Enterprise Server platform levert databases aan verschillende applicaties. De database servers zijn in een cluster opzet geïnstalleerd verspreid over de datacenters, waardoor bij uitval van een enkele SQL-server alle database functionaliteit door de tweede server wordt overgenomen. Als onderliggende besturingssystemen is Windows 2003 R2 Enterprise Edition gebruikt. De database en logfiles worden bewaard op gedeelde disks op het SAN/NETAPP. Bij uitval van één van de twee datacenters is een handmatige handeling noodzakelijk aan de storagezijde (polyserver) om een failover te volbrengen. Hiervan is ook het SQL cluster afhankelijk.

De clustermodus is in active/passive mode opgezet. Doorgaans kunnen gebruikmakende applicaties (ook de beheertools Citrix, Powerfuse, Softgrid, Altiris) geen gebruik maken van een tweede instantie (active/active). De SQL Resource is met een unieke NETBIOS in de WINS database en met de FQDN naam opgenomen in DNS van Active Directory. Het SQL-resource is als host-naam bereikbaar, maar komt niet voor als computer-object in Active Directory.

Voor de diverse applicaties wordt een minimale configuratie verzorgd ten behoeve van de beveiliging, bestaande uit een "sa" account (het root account van de sql system-administrator, SQL server user) die tijdens de SQL installatie wordt aangemaakt. Dit "sa" account mag niet worden gebruikt omdat hiermee de werking van andere databases en applicaties kan worden aangepast. Voor een applicatie wordt een eigen service account aangemaakt, welke vervolgens db-owner rechten krijgt. Rechten zodat een applicatie eigen databases kan aanmaken worden niet verstrekt. Als dit eenmaal gebeurd is, zullen de front-end applicaties gebruik maken van hun eigen



gegenereerde sql-accounts voor toegang tot het SQL-Cluster. Op deze manier is er geen uitgebreide configuratie nodig voordat de diverse front-end applicaties zichzelf kunnen installeren, en behoeft bij wijziging in de front-end applicatie versies geen wijziging plaats te vinden in de sql-configuratie.

Het SQL Cluster heeft opslag nodig voor de Quorum Disk, een Data disk en een Log disk, deze staan op een gedeelde disk die door beide SQL Cluster nodes tegelijkertijd wordt gebruikt. Op deze manier worden alle wijzigingen in de master node ook doorgevoerd zodat bij uitval van een locatie de slave-node toch nog alle benodigde databases kan benaderen.

2.2.1 Meer weten

Voor een volledige beschrijving wordt verwezen naar het Technisch Ontwerp versie 2.2.doc.



3. Rotterdamse richtlijnen

3.1 Informatiebeveiliging

Iedere nieuwe applicatie dient te worden geclassificeerd op de punten *vertrouwelijkheid* en *integriteit* om de eisen ten aanzien van informatiebeveiliging vast te stellen (zie **baseline Informatiebeveiliging**). Op basis van de gekozen classificatie zijn de volgende maatregelen noodzakelijk:

Vertrouwelijkheid:

Niveau	Authenticatie	Autorisatie	Monitoring	Beveiliging
Openbaar	Geen	Geen	Geen	Geen
Bedrijfs- vertrouwelijk	Authenticatie "basis" vereist. Sessie-timeout na 15 min inactiviteit. Voor klant absolute sessie-timeout na 120 min. Identiteit blokkeren na 3 achtereenvolgende foutieve authenticatie pogingen. Authenticatie "basis" nodig voor deblokkeren.	Autorisatie vereist (lid van organisatie).	Vastleggen herhaaldelijk foutieve authenticatie en tijdstip. Monitoring-gegevens bewaren voor periode van ½ jaar.	Outputvalidatie. Versleuteling tijdens transport buiten netwerk van Gemeente R'dam via transportbeveiliging of berichtbeveiliging. Kopieën van gegevens moeten net zo goed beveiligd worden. Gegevens uit productieomgeving worden niet gebruikt in OTA-omgevingen tenzij deze zijn geanonimiseerd en de geveenseigenaar toestemming heeft gegeven.
Vertrouwelijk	Authenticatie "midden" vereist. Sessie-timeout na 15 min inactiviteit. Voor klant absolute sessie-timeout na 120 min. Identiteit blokkeren na 3 achtereenvolgende foutieve authenticatie pogingen. Authenticatie "midden" nodig voor deblokkeren.	Autorisatie vereist (specifieke rol).	Vastleggen herhaaldelijk foutieve authenticatie en tijdstip. Monitoring-gegevens bewaren voor periode van 2 jaar.	Outputvalidatie. Versleuteling tijdens transport en op tussenstations binnen en buiten netwerk van Gemeente R'dam via berichtbeveiliging. Kopieën van gegevens moeten minimaal net zo goed beveiligd worden. Aantal kopieën minimaliseren. Berichtbeveiliging. Gegevens uit productieomgeving worden niet gebruikt in OTA-omgevingen tenzij deze zijn geanonimiseerd en de geveenseigenaar toestemming heeft gegeven.



Niveau	Authenticatie	Autorisatie	Monitoring	Beveiliging
Geheim	<p>Authenticatie "hoog" vereist.</p> <p>Sessie-timeout na 15 min inactiviteit. Voor klant absolute sessie-timeout na 120 min.</p> <p>Identiteit blokkeren na 3 achtereenvolgende foutieve authenticatie pogingen.</p> <p>Authenticatie "hoog" nodig voor deblokkeren.</p> <p>Geen SSO toegestaan.</p>	<p>Autorisatie vereist (specifieke rol).</p>	<p>Vastleggen correcte en foutieve authenticatie en tijdstip.</p> <p>Monitoring-gegevens bewaren voor periode van 7 jaar.</p>	<p>Output validatie.</p> <p>Versleuteling tijdens transport en op tussenstations via berichtbeveiliging. Versleutelde opslag van gegevens. Transport van gegevens minimaliseren. Alleen transport en opslag binnen vaste netwerk van Gemeente R'dam.</p> <p>Geen kopieën toegestaan behalve voor beschikbaarheid.</p> <p>Gegevens uit productieomgeving worden niet gebruikt in OTA-omgevingen tenzij deze zijn geanonimiseerd en de gegevenseigenaar toestemming heeft gegeven.</p>

Integriteit:

Niveau	Authenticatie	Autorisatie	Monitoring	Beveiliging
Niet zeker	Geen	Geen	Geen	Geen
Beschermd	<p>Authenticatie "basis" vereist.</p>	<p>Autorisatie vereist.</p>	<p>Vastleggen authenticatie (correct en foutief) en tijdstip.</p> <p>Vastleggen relevante input en output van een IT-systeem of service.</p> <p>Monitoring-gegevens bewaren voor periode van ½ jaar.</p>	<p>Input validatie.</p> <p>Controleren op mutatie tijdens transport.</p> <p>Transportbeveiliging of berichtbeveiliging.</p> <p>Gegevens: Versie van gebruikte gegevens is bekend.</p> <p>Na uitvoering van een service blijven gewijzigde gegevens consistent.</p>
Hoog	<p>Authenticatie "midden" vereist.</p>	<p>Autorisatie vereist.</p> <p>4-ogen principe vereist.</p>	<p>Vastleggen authenticatie (correct en foutief) en tijdstip.</p> <p>Vastleggen relevante input en output van een IT-systeem of service.</p> <p>Monitoring-gegevens bewaren voor periode van 2 jaar.</p>	<p>Input validatie.</p> <p>Controleren op mutatie tijdens transport.</p> <p>Berichtbeveiliging.</p> <p>Gegevens: Versie van gebruikte gegevens is bekend. Wijzigingen alleen op bron.</p> <p>Na uitvoering van een service blijven gewijzigde gegevens consistent.</p>
Absoluut	<p>Authenticatie "hoog" vereist.</p> <p>Geen SSO toegestaan.</p>	<p>Autorisatie vereist.</p> <p>4-ogen principe vereist.</p>	<p>Vastleggen authenticatie (correct en foutief) en tijdstip.</p> <p>Vastleggen relevante input en output van een IT-systeem of service.</p> <p>Monitoring-gegevens bewaren voor periode van 7 jaar.</p> <p>Vastleggen oude staat van te wijzigen gegevens.</p>	<p>Input validatie.</p> <p>Controleren op mutatie tijdens transport.</p> <p>Berichtbeveiliging.</p> <p>Gegevens: Gegevens worden niet buiten hun bron opgeslagen (behalve voor beschikbaarheid) en niet buiten hun bron gewijzigd.</p> <p>Na uitvoering van een service blijven gewijzigde gegevens consistent.</p>



3.2 Opensource en open standaarden

Het ICT-beleid is op dit punt aangescherpt en is erop gericht om bij nieuwe software ontwikkelingen, aflopende contracten of bij vervanging van bestaande software, eerst vast te stellen of er een adequate open source oplossing is.

Bij de keuze van software (ongeacht of dit open source of closed source software betreft) worden de volgende criteria toegepast:

- voorziet de software in de vereiste en gewenste functionaliteit
- worden open standaarden toegepast
- hoe lang is de software verkrijgbaar
- hoeveel gebruikers zijn er
- is de continuïteit van het onderhoud en de uitbreiding van de functionaliteit verzekerd
- past de software in de concerninformatiearchitectuur
- kan het bestaande beveiligingsniveau worden gehandhaafd bij gebruik van de software
- blijft het bereiken van een hoger beveiligingsniveau mogelijk
- is de kwaliteit van documentatie voldoende
- zijn er leveranciers die de invoering van software kunnen begeleiden
- wat zijn de totale kosten van aanschaf, aanpassing van hard- en software, conversie, opleiding gebruikers en beheerders
- wat zijn de kosten van beheer

Functionaliteit, kosten, open standaarden, continuïteit en beveiliging wegen het zwaarst in de beslissing over de verwerving en implementatie van software. Indien een open source produkt aan de gestelde eisen voldoet, wordt dit verworven.

Voor de opdrachtgever, projectleider, klant geldt:

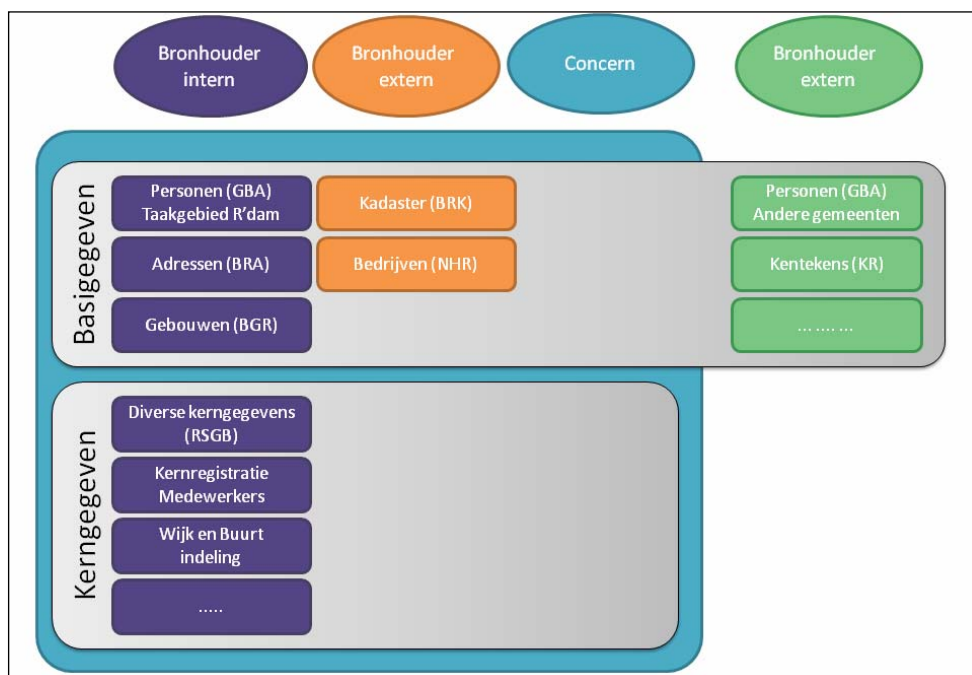
Een keuze voor een produkt dat niet aan de eis van open standaarden en open source software voldoet, dient te u kunnen motiveren en aangeven wanneer die keuze opnieuw wordt overwogen. Deze motivatie dient u aan te bieden aan CIO.

3.3 Gegevensuitwisseling

Binnen het Concern Rotterdam worden kerngegevens centraal beschikbaar gesteld in een aantal magazijnen. Gegevens uit deze magazijnen, maar ook uit andere concernsystemen, worden bij voorkeur aangeboden en onttrokken via de enterprise servicebus, de Rotterdamse gemeentelijke uitwisselingscomponent "GUC". Ter illustratie wordt hieronder kort het gegevensmagazijn en het GUC toegelicht.

3.3.1 Gegevensmagazijn

Het Gegevensmagazijn bevat alle basis- en kerngegevens van de gemeente Rotterdam en specifieke externe bronhouders. De volgende figuur maakt duidelijk welke gegevens dit zijn:



Wat doet het gegevensmagazijn wel?

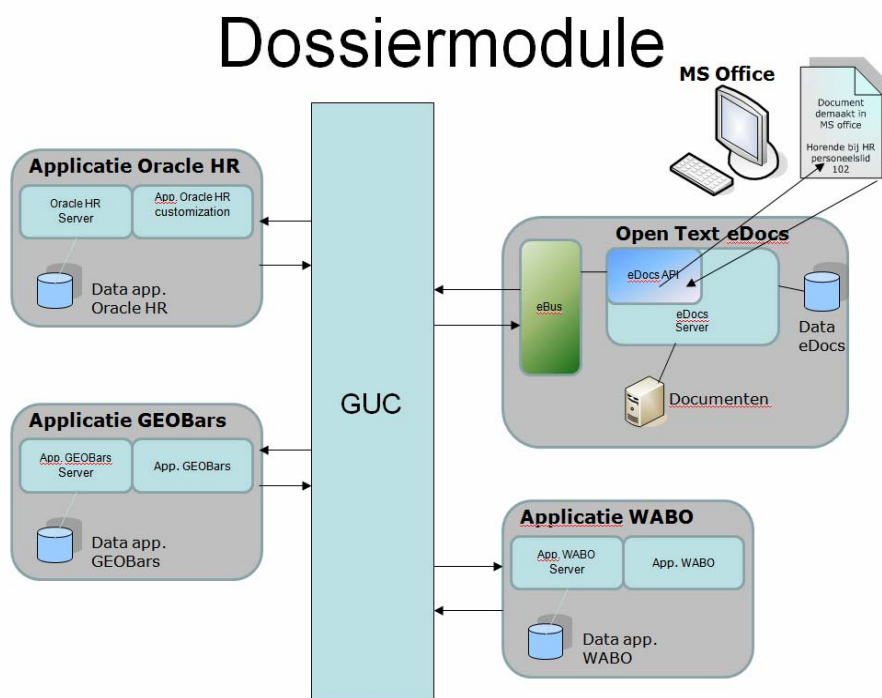
Het gegevensmagazijn doet wel
Bijwerken van gegevens in het gegevensmagazijn op basis van kennisgevingen van het stelsel
Filteren van informatie o.b.v. autorisatieniveaus
Auditing & logging
Aanbieden van services t.b.v. gegevensgebruik

Wat doet het gegevensmagazijn niet!

Het gegevensmagazijn doet niet!
Aanbieden van services voor gegevens buiten het stelsel basis- en kernregistraties
Orkestratie van services
Bijhouden van autorisatieniveaus

Bijvoorbeeld de personalia van de Rotterdamse jongeren kunnen uit het gegevensmagazijn worden onttrokken ten behoeve van het nieuwe systeem.

3.3.2 Gemeentelijke Uitwisseling Component GUC



Door de inzet van het product *Mule Community Edition* is voorzien in een gemeentelijke enterprise servicebus. Rotterdamse toepassingen kunnen door aansluiting op deze component gebruik maken van elkaars functionaliteiten en generieke en op maat gemaakte services. Een nieuwe toepassing dient gebruik te kunnen maken van deze GUC. De afspraken rondom het gebruik van de component zijn nog in ontwikkeling. De ontwikkelstandaarden rondom mule zijn neergelegd in *Ontwikkelstandaarden Mule v1.0*.

3.4 Gewenste Autorisatiemodel

De Gemeente Rotterdam hanteert de volgende richtlijnen ten aanzien van autorisatie en authenticatie:

Authenticatie en autorisatie van services wordt geregeld in de architectuurcomponenten Authenticatie en Autorisatie (P-GUC-1)

Voorzieningen, applicaties en services moeten gebruik maken van de standaard AA voorzieningen die de CIA biedt. (LDAP, WS-*, DigID, etc.). Dit betekent dat standaard commerciële applicaties hierop geselecteerd en ingericht moeten worden.

Voor ketenpartners wordt altijd met een zo "groot" mogelijke identiteit gewerkt.

De ketenpartner en/of het bedrijf is verantwoordelijk voor het beveiligen van toegang tot het juiste niveau en het intern zorg dragen van authenticatie en autorisatie. Dit zal formeel vastgelegd moeten worden als onderdeel van de SLA/contract.

Er worden geen “algemene” identiteiten gebruikt

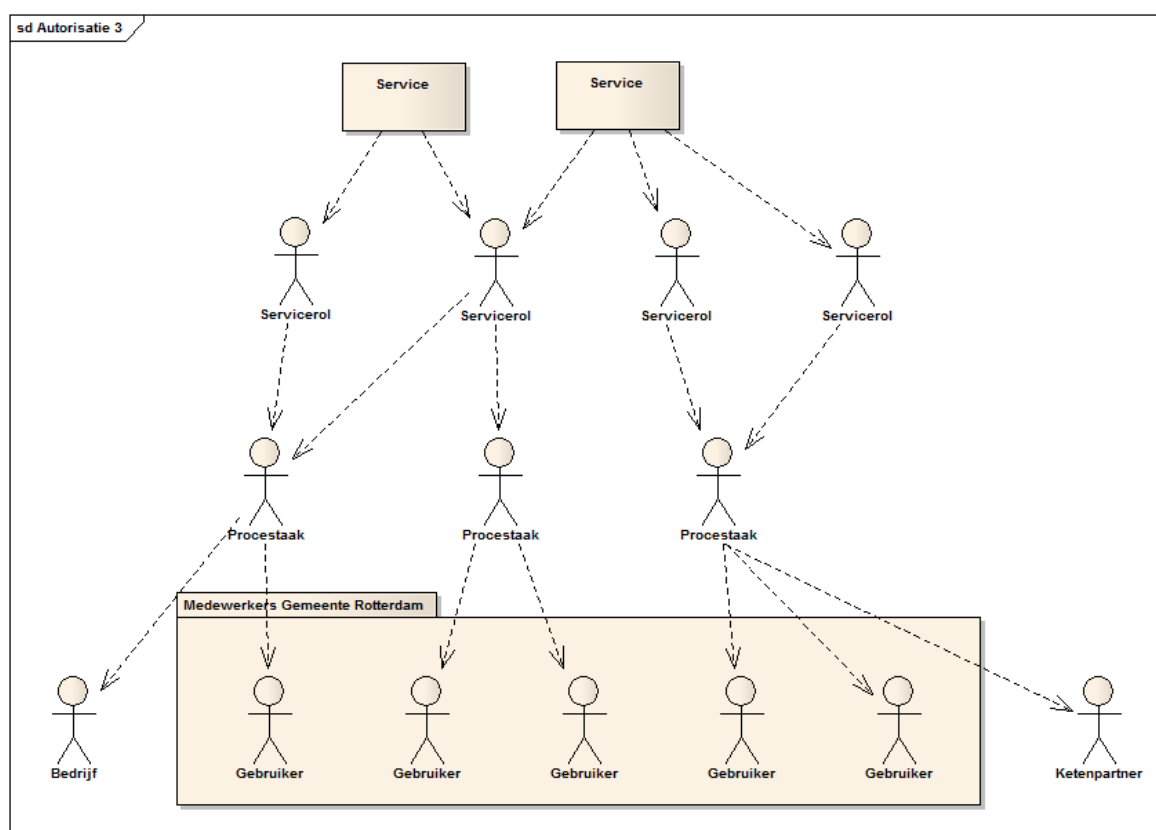
Er mogen geen identiteiten als stagiair of extern worden opgevoerd (wel rollen natuurlijk).

Gemeente Rotterdam streeft naar interne Single Sign On (SSO) en federatieve SSO (buiten de org.).

- Aansluiting op een externe SSO-voorziening is pas toegestaan nadat de security board advies heeft uitgebracht over deze voorziening en deze heeft bestempeld als “vertrouwd”.
- Dergelijke voorzieningen worden periodiek gecontroleerd.
- SSO neemt de verschillende authenticatie niveaus in acht.
- De GUC moet de gangbare SSO-protocollen/informatie kunnen doorgeven (SAML).
- SSO houdt zich aan de sessie-timeout zoals gedefinieerd voor authenticatie.

Het autorisatiemodel dient te worden gebaseerd op de volgende principes:

- Rollen, groepen, profielen, rechten worden gedefinieerd en beheert in het systeem;
- Gebaseerd op rollen;
- Transparant;
- Moet in staat stellen om werk uit te voeren (gebaseerd op taak), “just enough” autorisatie
- Flexibel, aanpasbaar (collega op vakantie, waarvan tijdelijk de taak overgenomen moet worden);
- Beheerlast minimaliseren;
- Gebruikersrollen moeten minimaal terugkomen.



Figuur 2.5.1. Gewenst autorisatiemodel: Procesgericht.

4. Acceptatiecriteria

4.1 Acceptatiecriteria technische infrastructuur en Rotterdamse richtlijnen

Code	Criterium	Meet eenheid	Norm
IR1	De applicatie dient zonder verlies van functionaliteit te functioneren binnen de gestelde IT-infrastructuur van de gemeente Rotterdam zoals beschreven in hoofdstuk 2	Ja/Nee	Ja
IR2	De applicatie(leverancier) dient gebruik binnen een Citrix en VMware omgeving te ondersteunen	Ja/Nee	Ja
IR3	De applicatie kan probleemloos persoonsafhankelijk via Citrix en Powerfuse worden gedistribueerd	Ja/Nee	Ja
IR4	Directe koppelingen tussen databases onderling zijn uitsluitend toegestaan binnen het Rotterdamse domein. Daarbij moet mogelijk zijn meerdere Microsoft domeinen te passeren.	Ja/Nee	Ja
IR5	Wachtwoorden mogen niet onversleuteld opgeslagen of getransporteerd worden.	Ja/Nee	Ja
IR6	Systeem is geschikt voor het principe single sign on op basis van netwerk ID voor interne medewerkers.	Ja/Nee	Ja
IR7	Het netwerkID wordt onttrokken aan de centrale LDAP – active directory dan wel een Oracle internet directory	Ja/Nee	Ja
IR8	In geval het een webapplicatie betreft dient deze device onafhankelijk te kunnen worden aangeboden (dus ook bruikbaar op PDA, smartphone, notebook, tablet, Ipad, e.d.)	Ja/Nee	Ja
IR9	Uw database dient zonder verlies van functionaliteit binnen het Oracle of SQL Platform te integreren zoals beschreven in paragraaf 2.2	Ja/Nee	Ja
IR10	Het niveau van vertrouwelijkheid en integriteit is bekend. De applicatie dient volledig aan de geschetste gegevensbeveiliging te voldoen en te implementeren zoals weergegeven in paragraaf 3.1	Ja/Nee	Ja
IR11	De applicatie voldoet aan de eisen voor opensource zoals beschreven in paragraaf 3.2	Ja/Nee	Ja
IR12	De applicatie kan probleemloos gegevens uitwisselen met het Rotterdams gegevensmagazijn middels een aansluiting op Mule, zoals beschreven in paragraaf 3.3	Ja/Nee	Ja
IR13	Het systeem werkt volgens het autorisatiemodel van de gemeente Rotterdam) middels een aansluiting op Mule, zoals beschreven in paragraaf 3.4	Ja/Nee	Ja
IR14	Het systeem kan koppelen aan zowel een Active directory als aan een Oracle internet directory t.b.v. centrale autorisatie en authenticatie	Ja/Nee	Ja
IR15	Bij grote voorkeur betreft het nieuwe systeem een webapplicatie welke gebruik kan maken van elders aangeboden webservices. Het nieuwe systeem biedt zelf tevens verrijkte informatie aan middels webservices ten behoeve van andere afnemende toepassingen.	Ja/Nee	Ja/Nee



Code	Criterium	Meet eenheid	Norm
IR16	Uitwisseling en koppeling met bronnen vindt zo veel mogelijk plaats op basis van webservices, orkestratie middels een 'Mule' enterprise servicebus (ESB). Binnen Rotterdam wordt soap-xml, StUF-BG 3.10 als standaard uitwisselingsformaat gebruikt.	Ja/Nee	Ja
IR17	Afspraken zijn gemaakt en vastgelegd met betrekking tot het gebruik en eigendom van broncode in geval van faillissement van de leverancier of wanprestatie van de leverancier.	Ja/Nee	Ja
IR18	Een door de applicatie geleverde (web)service bevat geen hard coded verwijzing naar resources (bijvoorbeeld een file adapter)	Ja/Nee	Ja
IR19	Meerdere instanties van één en dezelfde (web)service beïnvloeden elkaar niet.	Ja/Nee	Ja
IR20	Via het GUC aangeboden services dienen zich te conformeren aan de standaard foutafhandeling binnen het GUC.	Ja/Nee	Ja



5. Overdrachtcriteria intern IdR

5.1 Overdracht van software naar TAB

Code	Criterium	Meet eenheid	Norm
O1	De applicaties, componenten en onderliggende databases passen binnen het T.O. en voldoen aan de standaarden die gehanteerd worden binnen afdeling beheer van SSC ICT diensten. Afwijkingen van standaard worden goed gedocumenteerd en in de CMDB en de DVO opgenomen (ook de documentatie).	Ja/Nee	Ja
O2	Per applicatie wordt er een dossier aangeleverd met media, handleidingen (installatiehandleiding, beheerdershandleiding, gebruikersdocumentatie, intakedocument en architectuurtekening) en overige relevante informatie. Deze dossiers worden opgenomen in de DSL en opgeslagen in de Processmanager (onderdeel van de CMDB).	Ja/Nee	Ja
O3	Backup & Recovery is geregeld en getest.	Ja/Nee	Ja
O4	De applicatie (en onderliggende servers en databases) is opgenomen in de daarvoor aanwezige monitoring tools	Ja/Nee	Ja
O5	Alle licenties zijn ingekocht en worden beheerd door Bedrijfsvoering.	Ja/Nee	Ja
O6	De KSO's werken in een (door de leverancier) gecertificeerde omgeving en worden ondersteunt door de leverancier.	Ja/Nee	Ja
O7	Leveranciergegevens zijn bekend en ingevuld in de CMDB	Ja/Nee	Ja
O8	Lijst van gebruikers is bekend en ingevuld in de CMDB.	Ja/Nee	Ja
O9	Er zijn DVO's met zowel de klant als met de leverancier.	Ja/Nee	Ja
O10	Er is een (realistische) verwacht aantal incidenten en verwachte beheerslast bekend.	Ja/Nee	Ja
O11	De sources van de KSO zijn (eventueel via ESCROW) beschikbaar voor ICT Service.	Ja/Nee	Ja
O12	De FAB, TAB, eigenaar en relaties met andere CI's van de KSO is bekend en benoemd in de CMDB.	Ja/Nee	Ja
O13	Er is kennis aanwezig (of kan vergaard worden) van de onderliggende technieken De CMDB is volledig ingevuld.	Ja/Nee	Ja

Bijlagen

Beheermodel

In onderstaand bestand zijn de taken per beheervorm toegelicht:



Beheermodel.doc

Standaard intakelijst



H:\bijbel\Template
Intake Technisch App